Request Manager Installation and Configuration Guide

vCloud Request Manager 1.0.0

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-000475-00

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About This Book 5

1 About vCloud Request Manager 7
- Request Manager Components 7
- How Request Manager Uses Network Ports 11
- Preparing to Use Request Manager 11
- Installation Planning Worksheet 12
- Finding More Information 13

2 Request Manager System Requirements 15
- System Requirements 15
- Oracle Configuration 17
- Performance and Scalability 18
- Security 19

3 Installing Request Manager 21
- Installation Process Overview 21
- Install Request Manager 21
- Configure Request Manager 22

4 Accessing Request Manager 27
- Access the Request Manager Admin Portal 27
- Access the Request Manager Admin Portal without Active Directory 28
- Access the Request Manager User Portal 28

5 Administration Overview 31
- Active Directory 31
- Request Manager Roles 35
- Connecting to Multiple Instances of VMware vCloud Director 37
- Incoming Email Server 44
- Workflow Management 47
- Cloud Blueprints 57
- Defining Providers 59
- Polling Service 60

6 About Software License Management 61
- Understanding Licenses 61
- Create a Software Product 61
- Edit a Software Product 62
- Delete a Software Product 62
- Add License Information to a Software Product 63

Defining Software Products Options 63
Viewing Software License Allocation 65
Associating Software Products with vApp Templates 66

Index 69

About This Book

This manual, the *VMware vCloud Request Manager Installation and Configuration Guide*, provides information about installing and configuring vCloud Request Manager.

Intended Audience

This manual is intended for anyone who needs to install and configure vCloud Request Manager. The information in this manual is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

Technical Support and Education Resources

The following technical support resources are available to you. To access the current version of this book and other books, go to http://www.vmware.com/support/pubs.

Online and Telephone Support

To use online support to submit technical support requests, view your product and contract information, and register your products, go to http://www.vmware.com/support.Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to http://www.vmware.com/support/phone_support.html.

Support Offerings

To find out how VMware support offerings can help meet your business needs, go to http://www.vmware.com/support/services.

VMware Professional Services

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to http://www.vmware.com/services.

About vCloud Request Manager 1

vCloud Request Manger is a Web-based application that is an add-on to vCloud Director. Request Manager identifies the clouds and vApps managed by vCloud Director.

vCloud Request Manager provides enhanced governance and control of private cloud infrastructures based on vCloud Director. Request Manager:

- Adds sophisticated approval workflows to provisioning requests
- Automatically tracks software license usage
- Enforces standardized settings on cloud partitions

This chapter includes the following topics:

- "Request Manager Components," on page 7
- "How Request Manager Uses Network Ports," on page 11
- "Preparing to Use Request Manager," on page 11
- "Installation Planning Worksheet," on page 12
- "Finding More Information," on page 13

Request Manager Components

Architecture

vCloud Request Manager layers over the top of vCloud Director and communicates with it primarily through the vCloud API. In this way, a single instance of vCloud Request Manager can support multiple private clouds and even public cloud providers, delivering a unified end user portal and request management across a hybrid cloud.

Figure 1-1. High-Level Request Manager Architecture

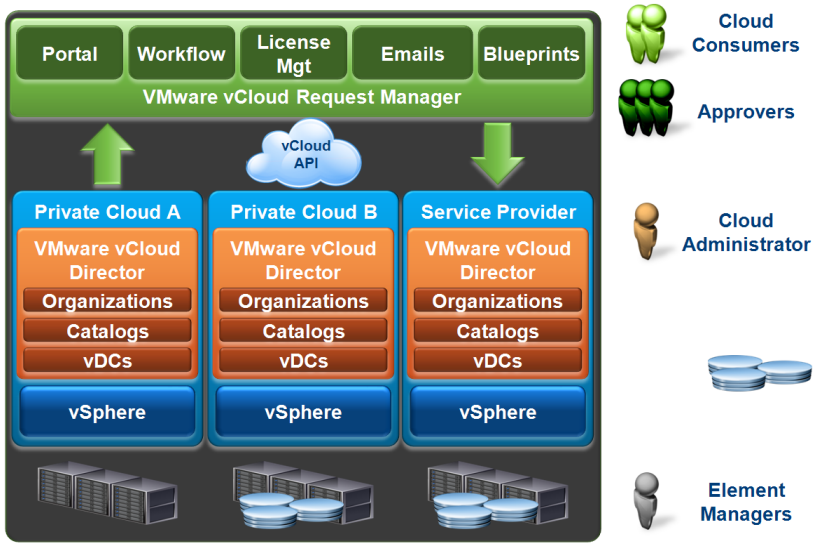
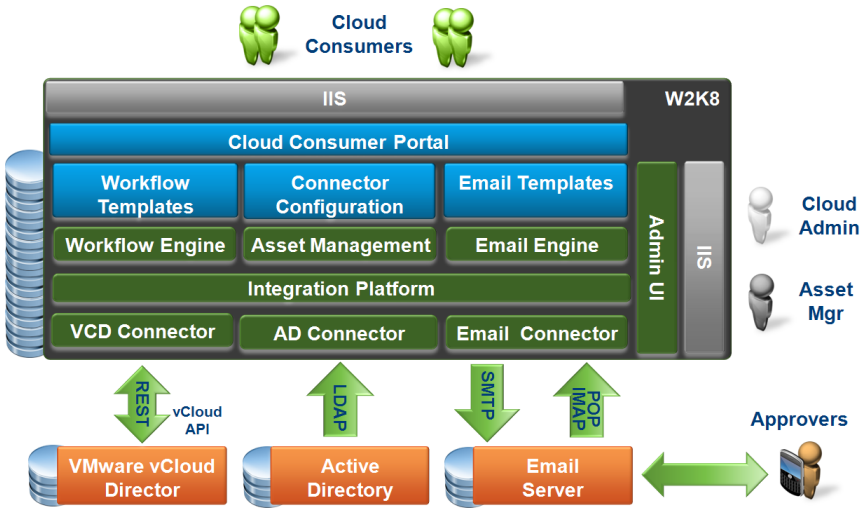


Figure 1-2. Detailed Request Manager Architecture



Users

Request Manager users can include the following.

vCloud Administrator The vCloud Administrator is the administrator responsible for Request Manager configuration after installation. The administrator is responsible for assigning security roles to cloud Blueprint Administrators and Asset Manager users, troubleshooting workflow tasks that fail to complete because of system errors, creating or editing workflow tasks to accommodate company-specific approval processes, and managing integrated sources.

Blueprint Administrator The Blueprint Administrator manages cloud blueprints, including creating and editing cloud blueprints. The Blueprint Administrator also manages Provider CIs, including creating and editing Providers and specifying the vCloud Director source, provider network, and the vCloud Director for that Provider CI.

Manager The users who create private cloud partitions. Users can include development managers, QA managers, pre-sales managers, and training managers.

Engineer The users who create individual virtual machines and virtual appliances. Users can include QA Engineers, pre-sales engineers, developers, trainers, etc.

Asset Managers The user responsible for registering the available software licenses.

See "Request Manager Roles," on page 35 for information about Request Manager user roles and permission.

Software Components

Request Manager requires the following software components.

- An Oracle database.
- An Active Directory server.

- One or more instances of vCloud Director.
- A dedicated email account.

Oracle Database The installation requires access to an Oracle database server that is configured to meet specific requirements to support Request Manager.

Active Directory Server Request Manager populates its users by accessing the same Microsoft Active Directory domain that is used by vCloud Director. In a default install, Request Manager's Active Directory server should be located within the same domain as vCloud Director's. Active Directory integration requires there is an existing single group or organization unit within the directory to which every user belongs. For example, Domain Users.

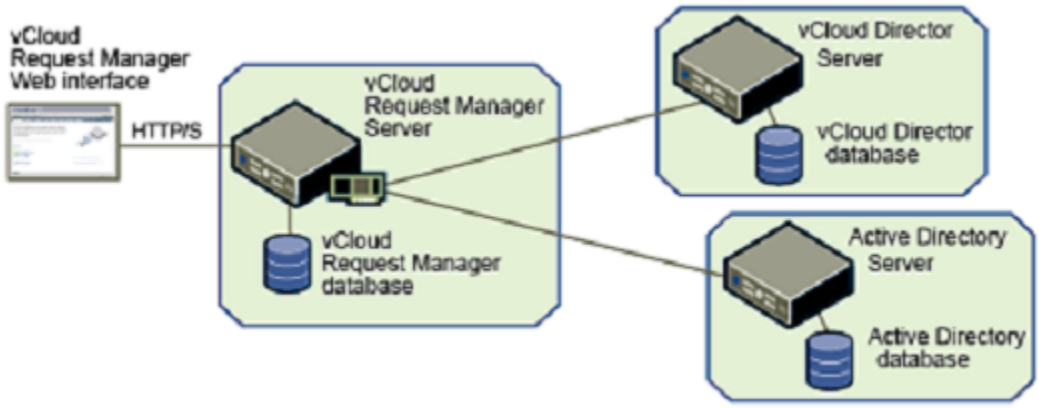
vCloud Director VMware vCloud Director must be installed (on another server within the domain) before Request Manager can be configured. An account with vCloud system administrator privileges must be pre-configured for Request Manager to use. Request Manager cannot use an account created for a specific vCloud organization.

Email Server Request Manager uses an assigned email account on a email server. It connects to the email server to send emails using SMTP and retrieves emails sent to it using POP3 or IMAP.

Basic Deployment

The following graphic illustrates the Request Manager, vCloud Director, and Active Directory components and how they are connected.

Figure 1-3. Request Manager Basic Deployment



User Interfaces

Request Manager uses the following interfaces:

Request Manager User Portal	The portal used by engineers and cloud owners to request new clouds and provision new virtual applications.
VMware Service Manager	The administration user interface, used by administrators and asset managers to manage workflow, forms, email, and connector mappings. Throughout this document, this interface will be referred to as the Request Manager Admin Portal.
VMware vCloud Director	Populates Request Manager cloud data and provides the interface, automation, and management required by enterprises and service providers to build private and public clouds.

How Request Manager Uses Network Ports

The Request Manager server uses network ports to communicate with vCloud Director, the Oracle database, and the email server used for incoming and outgoing traffic.

No configuration is required unless the servers or database is not using a default port. In that case, you will need to open the port for Request Manager access. If any of these ports are in use by other applications or are blocked on your network, you must reconfigure Request Manager to use different ones.

The following table lists the default Request Manager port access connections.

Table 1-1. Request Manager Port Access Requirements

Port Number	Direction of Traffic	Description
1521	Outgoing	Oracle port
25	Outgoing	Outbound E-mail server port for SMTP
110	Outgoing	Inbound E-mail server port for POP3
143	Outgoing	Inbound E-mail server port for IMAP
80	Incoming	Inbound HTTP for Request Manager user
80	Outgoing	Outbound REST (HTTP) for VMware vCloud Director
389 (non SSL)	Outgoing	Outbound Active Directory using LDAP
636 (SSL)	Outgoing	Outbound Active Directory using LDAP over SSL

Preparing to Use Request Manager

Prepare your environment before you install Request Manager.

An environment that is ready for Request Manager includes the following:

- An Oracle Database 10g or higher (10.2.0.4+) server that is ready for use.
- Access to a vCloud Director Server that is populated with at least one published catalog.
- Access to the same Microsoft Active Directory domain that is used by vCloud Director.
- Roles and permissions are identified for the administrators and users who will install, configure, and manage Request Manager.

Installation Planning Worksheet

Use the deployment planning worksheet to record your choice of server system, database, and optional components for a production environment.

Component	Considerations	Decision
vCloud Director		
vCloud Director	Determine the vCloud Director server Request Manager will connect to. The vCloud Director server must be compatible with Request Manager. See Chapter 2, "Request Manager System Requirements," on page 15.	Compatible with vCloud Director?
vCloud Director URL	Determine the URL of the vCloud Director instance to which Request Manager will connect.	URL?
vCloud Director user name and password	You must have the administrator user name and password for the vCloud Director instance to which Request Manager will connect. vCloud Director requires that the user name must be fully qualified by vCloud Director organization and that organization must be System. For example, `administrator@system`.	Fully-qualified user name? Password?
vCloud Director User	The vCloud Director user must have system wide privileges.	System wide privileges?
Database		
Database Server	Determine the database Request Manager will use. The database server must be compatible with Request Manager. See Chapter 2, "Request Manager System Requirements," on page 15.	Oracle database version?
Configure the database	The database must be configured before installing Request Manager. See "Oracle Configuration," on page 17.	Is the database configured?
Database TNS	The TNS of the database Request Manager will use.	Database TNS?
Database user name and password	You must have the administrator user name and password for the Oracle database Request Manager will use.	User name? Password?
DBA Privileges	The database user must have the required privileges. See "Oracle Configuration," on page 17.	Correct privileges?
Active Directory		
Active Directory URL	The URL of the Active Directory Request Manager will synchronize with.	URL?
Active Directory user name and password.	You must have the administrator user name and password for the Active Directory Request Manager will use.	User name? Password?
Email server		
Email server for outgoing mail	Connection information for the email server used for outgoing email.	Port number? Host name?
Email server user name and password	You must have the user name and password for the email account.	User name? Password?
Email server for incoming mail	Connection information for the email server used for incoming mail.	Port number? Host name? Protocol?
Network		
Port Number Assignments	Make sure that the default ports used are available for Oracle, vCloud Director, and inbound and outbound email servers. See "How Request Manager Uses Network Ports," on page 11.	Port numbers used?

Component	Considerations	Decision
Request Manager Roles		
Users and Roles	Identify the users who will be assigned as vCloud Director Admins, Blueprint Admins, and Asset Manager. See "Request Manager Roles," on page 35.	Users and roles?

Finding More Information

You can access all vCloud Request Manager documentation online at http://www.vmware.com/support/pubs/vrm_pubs.

In addition to this guide, documentation for this product includes the following:

- The Request Manager 1.0 Release Notes provide product overview and a description of known issues.
- The *VMware vCloud Request Manager User's Guide* provides a product overview and general tasks for end users.

Request Manager System Requirements 2

This section includes information on the System Requirements for Request Manager 1.0.0.

This chapter includes the following topics:

- "System Requirements," on page 15
- "Oracle Configuration," on page 17
- "Performance and Scalability," on page 18
- "Security," on page 19

System Requirements

Request Manager is compatible with the following VMware releases, servers, browsers, operating systems, and databases.

vCloud Director

Request Manager requires vCloud Director 1.0.

The following lists the system requirements for vCloud Director.

- A vCloud Director installation on another server within the domain.
- An pre-configured account within vCloud Director with full system administrator privileges. This account must not belong to a specific vCloud Director organization.

  NOTE VMware recommends that this is a dedicated account. Shared accounts are supported, however assigning a dedicated account enables Request Manager actions to be more clearly distinguished within vCloud Director.

- vCloud Director is configured with at least one published catalog that contains a set of enterprise-approved vApp templates.

  NOTE If there are no published catalogs, users in new clouds will not be able to create new applications.

Microsoft Active Directory

Request Manager requires Microsoft Active Directory 2003 or 2008. The Request Manager server must belong to the domain that is administered by the Active Directory server.

Request Manager populates its user database by scanning the domain and matching those users to users defined within vCloud Director. A user must belong to this domain in order to access the Request Manager User Portal. Request Manager will only recognize users within vCloud Director who have been imported from this domain.

The following vCloud Director users will not be recognized by Request Manager:

- Manually created users; that is users who have not been imported from the domain.
- Users imported from an alternative domain.

NOTE Request Manager does not support OpenLDAP.

Email Server

Request Manager requires a dedicated email account. The following lists the system requirements for the email server.

- A dedicated email account that is new and not shared with any existing user or application.
- SMTP to send emails from that account.
- POP3 or IMAP to receive email notifications sent to that account.

Request Manager Web Server

- Operating System: Microsoft Server 2008 R2 64-bit
- Internet Server: IIS 7
- Hardware: 2.8 GHz CPU and 4 GB RAM
- Miscellaneous: Microsoft .NET Framework 3.5 SP1

NOTE You can install Request Manager on a physical machine or a virtual machine, as long as it meets these system requirements.

Request Manager Admin Portal

The Request Manager Admin Portal supports the following operating systems and browsers.

Table 2-1. Request Manager Admin Portal Support

Operating System	Browsers
Windows XP SP3	Internet Explorer 7 and 8
Windows Vista	Internet Explorer 7 and 8
Windows 7	Internet Explorer 7 and 8

Request Manager User Portal

The Request Manager User Portal supports the following operating systems and browsers.

Table 2-2. Request Manager User Portal Support

Operating System	Browsers
Windows XP	Internet Explorer 7 and above, Mozilla Firefox 3 and above, and Chrome 4.0 and above
Windows 7	Internet Explorer 7 and above, Mozilla Firefox 3 and above, and Chrome 4.0 and above

Table 2-2. Request Manager User Portal Support (Continued)

Operating System	Browsers
Mac OS 10	Safari 4.0 and above
iPad	Safari 4.0 and above

Supported Database Software

Request Manager 1.0.0 supports only Oracle Server databases. The following lists the system requirements for the Request Manager database. See "Oracle Configuration," on page 17 for more information on database configuration requirements.

- 2 CPUs
- At least 50 GB of available disk space

The following lists the Oracle databases supported for use as the Request Manager database.

Table 2-3. Oracle Database Support

Oracle Server Version	Oracle Client Version
Oracle 10g Standard edition, release 2, version 10.2.0.4+, 32-bit and 64-bit	10.2.0.4+, 32-bit
Oracle 10g Enterprise edition, release 2, version 10.2.0.4+, 32-bit and 64-bit	10.2.0.4+, 32-bit
Oracle 11g Standard edition, release 1, version 11.1.0.7+, 32-bit and 64-bit	11.1.0.7+, 32-bit
Oracle 11g Enterprise edition, release 1, version 11.1.0.7+, 32-bit and 64-bit	11.1.0.7+, 32-bit

Oracle Configuration

An Oracle Server and Oracle Client must meet specific requirements to support Request Manager.

Oracle Server Configuration

Oracle Server has the following configuration requirements when used as the Request Manager database.

- Request Manager requires access to an Oracle database server.
- The character set of that server must be set to UTF-8 to support Unicode (i18n) characters.
- The Oracle and Request Manager servers must be configured to operate in the same time zone and have the same server time.
- Request Manager can share an existing Oracle database server, provided that:
  - The existing server's pre-requisites must meet those of Request Manager.
  - Other applications using the database support the same configuration.
  - Applications must be configured with adequate resources.

  NOTE Multiple applications sharing a single Oracle server can compete for server resources. The Oracle DBA must configure applications to have the resources they need (For example, increase the connection limit; move databases to separate servers). During heavy loads, some resources may not be available (For example, the max number of connections may be exceeded) and can result in application errors.

- The Oracle DBA must configure a new Oracle user with a dedicated schema for Request Manager with the following minimum privileges:
  - CONNECT
  - CREATE TABLE
  - CREATE PROCEDURE
  - CREATE TRIGGER
  - CREATE TYPE
  - CREATE VIEW
- The Oracle DBA must set up a TNS configuration to the database on the Request Manager server.

Oracle Client Configuration

The installation requires the 32-bit edition of the Oracle client software to be present on the Request Manager server. The 32-bit edition should be used even if the operating system is 64-bit. Request Manager may experience problems on servers where the 64-bit edition of the client software is installed or has been previously installed.

Performance and Scalability

This section provides scalability information for sizing.

Scanning LDAP

Scanning large sites can take a long time. The following test data provides some idea of how long scans can take.

- First time scans of an Active Directory server with 60,000 users completed in approximately 8 hours.
- Subsequent scans of the same server (updating only changed records) completed in less than half an hour.
- Subsequent scans of the same server (updating all records) completed in approximately 8 hours.

LDAP updates are reflected when the next scheduled scan is run.

See "Active Directory," on page 31 for more information about configuring and synchronizing Active Directory.

Scanning vCloud Director

Scanning a large number of vApps and resources can take a long time. The following test data provides some idea of how long scans can take.

Table 2-4. Average Scan Times for vCloud Director Scans

	Typical	Extreme	Time Taken (Extreme)
Organizations per Private Cloud	5	100	3.7 sec/resource
Members per Organization	20	500	0.3 sec/resource
Catalogs per Organization	2	10	0.8 sec/resource
Catalog Items per Catalog	50	100	1.0 sec/resource
Total Running vApp Instances per vCloud Director Instance	100	5000	2.1 sec/resource
Running vApp Instances per Organization	50	500	2.1 sec/resource

Based on these average scan times, scanning 100 vApps can take 4 minutes. Scanning 5000 vApps can take 3 hours.

Scan updates are reflected when the next scheduled scan is run. By default, scans are set to run hourly. See "Create or Modify a vCloud Director Synchronization Schedule," on page 40.

Request Manager maintains a cached copy of the data within vCloud Director for better responsiveness. This cache is populated by scheduled scans and is only as current as the latest scan. An exception is the status display of each vApp, which is retrieved live from vCloud Director.

NOTE vCloud Director permits consumers of the vCloud API to be logged in for maximum period of 24 hours. If a scheduled scan of vCloud Director by Request Manager were to take longer than 24 hours, Request Manager's session would expire and the scan would abort without completing. However, a new scan would begin shortly after and resume where the previous scan had completed.

Database Sizing

Running a scan on a large number of vApps and resources can consume a lot of database space. The following test data provides some idea of how much space.

- Scanning 30,000 resources consumes approximately 270 MB, or 9.21 KB/resource.
- A scan of 100 vApps can consume 1 MB. A scan of 5000 vApps can consume 45 MB.

Security

Security certificates must be manually installed.

Security Certificates

Request Manager communicates with vCloud Director over a secure connection with SSL. Optionally, Request Manager can communicate with the Active Directory server using SSL. Communication over SSL can only succeed if the Request Manager server is able to trust the certificates utilized by those servers.

A server's certificate will be trusted by the Request Manager server if it meets the following prerequisites:

- The certificate or the certificate of its issuer must be installed to the Trusted Root Certificate Authorities store for the local machine. See "Installing a Security Certificate," on page 20 for directions on how and where the certificate should be installed.
- The certificate must be issued to either the host name (fully qualified by domain) of the remote server or the domain to which it belongs. For example, **`server1.mydomain.com`** or **`mydomain.com`**. Furthermore, when connecting via SSL the same fully qualified host name must be specified in the Active Directory Connection String or the vCloud Director server URL.
- The certificate be valid and must not have expired.

NOTE If either of the Active Directory or vCloud Director server certificates have not been issued to fully qualified host name, these certificates will need to be re-issued on those servers by the administrator of those servers. Please consult the documentation for these products for instructions on how to re-issue these certificates.

Installing a Security Certificate

Request Manager requires a security certificate to connect to VMware vCloud Director. Optionally, Request Manager can communicate with the Active Directory server over SSL. In these cases, you must install a security certificate to ensure successful communication.

Prerequisites

See "Security," on page 19.

Procedure

1 Open the Control Panel and select **Internet Options**.

2 Open Internet Options and select **Content**.

3 Click **Certificates**.

4 Select **Trusted Root Certification Authorities** and click **Import**.

5 Click through the Certificate Import Wizard.

6 At the Certificate Store screen, select **Place all certificates in the following store** and click **Browse**.

7 Click **Show physical stores**.

8 Expand the certificates store and select **Local Computer**.

9 Click **OK**.

This closes the window.

10 Complete the wizard.

The security certificate is installed.

What to do next

Continue with the installation of VMware Request Manager.

Security Certificate Warnings

During installation, the Configuration Wizard will attempt to test whether it can establish a connection over SSL with the specified connection parameters.

If a connection fails, a dialog will be displayed detailing the reasons why the connection could not be trusted and suggest actions that could be taken to resolve those issues. In addition, the dialog provides options to inspect and install the certificates issued by the server.

It is strongly advised that you consult with the relevant system administrators before directly installing a certificate with this dialog to avoid the server trusting compromised connections. It always best practice for the certificate of a remote server to be manually provided by that server's administrator rather than downloaded from the server.

Cookies

The Request Manager portal identifies the existing cookie security settings configured for the Request Manager server.

The portal stores the transient session ID, but no client sensitive information is stored. The Request Manager portal does not require a cookie to work. It only provides a mechanism to confirm a user does not attempt to impersonate another user by borrowing their session ID.

3 Installing Request Manager

Installation includes running the vCloud Request Manager installation executable, configuring the database, and configuring the vCloud Director, Active Directory, and email server settings.

This chapter includes the following topics:

- "Installation Process Overview," on page 21
- "Install Request Manager," on page 21
- "Configure Request Manager," on page 22

Installation Process Overview

Understand the deployment process before you install and configure vCloud Request Manager. An overview of the initial setup steps required to install vCloud Request Manager includes the following.

Complete the Installation Planning Worksheet. See "Installation Planning Worksheet," on page 12.

Download and run the installation executable. See "Install Request Manager," on page 21.

Use the configuration wizard to configure the database, vCloud Director, Active Directory, and email server settings. See "Configure Request Manager," on page 22.

Open a browser and log in to Request Manager with the URL: `http://<hostname>/portal`. See "Access the Request Manager User Portal," on page 28.

Install Request Manager

VMware vCloud Request Manager software is distributed as an executable file named **`vmware-vcloud-request-manager-x.x.x-nn.exe`**, where *x.x.x* represents the version number and *nn* represents the build number.

Prerequisites

You must understand the installation process and the system requirements before you install Request Manager.

Procedure

1. Right-click the installation file, **`vmware-vcloud-request-manager-x.x.x-nn.exe`**, and select **Run as administrator**.

   The User Account Control window displays.

2. Click **Yes** to authorize the Request Manager application to make changes to your computer.

   The InstallShield Wizard window displays and lists the items that are required to be installed on your computer.

3 Click **Install.**

Request Manager installs Visual JSharp .NET Redistributable Package 2.0 on your computer.

The Welcome screen appears.

4 Click **Next** to continue with the installation of Request Manager.

After you click **Next**, the vCloud Request Manager License Agreement window displays.

5 Select the option **I accept the terms of the license agreement** and click **Next**.

6 Enter your username and company name and click **Next**.

7 Select the setup type **Complete** and click **Next**.

The Ready to **Install the Program** screen displays.

8 Click **Install** to begin the installation.

The InstallShield Wizard installs Request Manager and displays the InstallShield Wizard Complete screen.

9 Click **Finish** to complete the installation.

Request Manager is installed on your computer. After the installation is complete, the installer launches the vCloud Request Manager Configuration Wizard.

What to do next

Click **Next** to start the vCloud Request Manager Configuration Wizard. Configure the Request Manager using the configuration wizard. See "Configure Request Manager," on page 22.

Configure Request Manager

You can configure Request Manager using the configuration wizard. The installer launches the vCloud Request Manager Configuration Wizard.

Prerequisites

You must supply the following information during the installation.

Oracle Database:

- The TNS name of the database Request Manager will use.
- The hostname of the database Request Manager will use.
- A user name and password for the database Request Manager will use.
- If you want to connect to an existing database, make sure that you initialize the database to remove all existing stored database information.

Email Configuration:

- The outgoing email server connection information.
- The user name and password of the email server.
- The incoming email server connection information.

Microsoft Active Directory:

- The hostname or IP address of the AD Server.
- The user name and password of the AD administrator.

VMware vCloud Director:

- The hostname of the vCloud Director Server.
- The fully-qualified user name and password of the vCloud Director administrator.
- Install the vCloud Directory security certificate. See "Installing a Security Certificate," on page 20.

The wizard can be cancelled at any point, but it generally should only be run once. Re-launching the wizard will not create a new database, and the out-of-the-box configurations will overwrite any configurations in the existing database that the user may have already specified. The user can opt to point the wizard to use a different, new, clean database however.

Re-launching is recommended to complete an interrupted configuration; it is not recommended for use as a means to perform subsequent modifications to those configurations. These modifications should be performed using the Request Manager Admin Portal. See Chapter 5, "Administration Overview," on page 31.

Procedure

1 From **Step - 1 Welcome**, click **Next** to start the wizard.

The **Step - 2 Configure Database Connection** screen appears.

2 Specify the connection parameters to the vCloud Request Manager database.

a Enter the TNS for the database.

The TNS must be 32-bit.

b Enter the user name and password for the database.

3 Click **Test Connection** to test the connection to the database.

If the connection succeeds, a confirmation appears.

4 Click **Next** to continue.

The **Step - 3 Building Database** screen appears. The configuration wizard creates and populates the database.

5 Click **Next** to continue.

The **Step - 4 Configure Email Server** screen appears.

6 Configure the outbound email server.

a Enter the port number.

b Enter the full domain name of the mail server.

c Enter the user ID and password for the mail server.

7 Configure the inbound email server.

   a Select the protocol to use.

   b Enter the port number.

   c Select **Reuse outbound server configuration** to populate the remaining fields with the information entered in the outbound email server fields.

   d Enter the full domain name of the mail server.

   e Enter the user ID and password for the mail server.

   f Enter a dedicated email address to use for email notifications.

   g Select **Skip this step** to continue to the next configuration wizard screen.

   If you choose to skip email configuration, configure email server settings using the Request Manager Admin Portal. See "Incoming Email Server," on page 44.

8 Click **Next** to continue.

   The **Step 5 - Configure Active Directory Server** screen appears.

9 Configure the Active Directory Server.

   a Enter the LDAP Connection String.

   If you have large numbers of users in your organization (for example, tens of thousands), it is recommended that you adjust this LDAP connection string to restrict the users of vCloud Request Manager to a subset of your organization's users. See "Configure Active Directory," on page 32.

   b Enter the user name and password.

   c Select the connection setting as **Server Bind**, **NTLM**, or **SSL**.

   d Enter the NT Domain Name.

   e Select **Skip this step** to continue to the next configuration wizard screen.

   If you choose to skip Active Directory Server configuration, configure Active Directory server settings using the Request Manager Admin Portal. See "Active Directory," on page 31.

10 Click **Next** to continue.

   The **Step 6 - Configure vCloud Director Server** screen appears.

11 Configure the vCloud Director Server.

   a Enter the URL of the vCloud Director Server.

   Make sure to include **`https://`** as part of the URL. Do not include any path information that would access the vCloud Director console. For example, do not include **`/vcloud`** or **`/vcloud/myorg`** in the URL.

   b Select **by-pass proxy settings** to ignore any configured proxy settings.

   Occasionally proxy settings may prevent a connection being successfully established. Sometimes performance can vary depending on whether proxy settings are used or not.

   c Enter the user ID and password for the vCloud Director administrator.

   vCloud Director requires that the user name must be fully qualified by vCloud Director organization and that organization must be System. For example, `administrator@system`.

   d Select **Skip this step** to move to the next configuration screen.

   If you choose to skip vCloud Director Server configuration, configure vCloud Director Server settings using the Request Manager Admin Portal. See "Connecting to Multiple Instances of VMware vCloud Director," on page 37.

12 Click **Next** to continue.

The **Step 7 - Configure System Identity** screen appears.

13 Configure system identity information.

a Specify an email address for system notifications.

b Create a password for the administrator account and then confirm the password you created.

This password is required to log in to the Admin portal when there are no administrator accounts in Active Directory. See "Access the Request Manager Admin Portal without Active Directory," on page 28.

14 Click **Next** to continue.

The **Step 8 - Synchronization Options** screen appears.

15 Click **Next** to continue.

The **Step 9 - Starting Services** screen appears and displays a progress bar.

16 Click **Next** to continue.

The **Step 10 - Synchronization Progress** screen appears and displays the status of the Active Directory and vCloud Director synchronization, including the number of Active Directory users and number of vCloud Director resources and links. After the synchronization is complete, the **Step 11- Define Administrators** screen appears.

NOTE The synchronization time varies depending on the size of the Active Directory and vCloud Director resources. See "Performance and Scalability," on page 18. If the synchronization fails to complete, proceed and complete the configuration wizard and refer to "View vCloud Director Synchronization Activity," on page 42 for information about how to view synchronization log information on Request Manager Admin Portal. You can then execute a subsequent scan using Request Manager Admin Portal by creating a new synchronization schedule. See "Create or Modify a vCloud Director Synchronization Schedule," on page 40 and "Create or Modify an Active Directory Synchronization Schedule," on page 33.

---

17 Define the system administrators.

a Enter a user name to add Request Manager administrators.

Enter a user name or click **Search** to find and select a name from the Active Directory.

b Click **Add** to add the user.

c Select a role for each user you add.

At least on user must be assigned the Admin role.

d (Optional) To remove a user, select a user name from the Selected list and click **Remove**.

18 Click **Next** to continue.

The **Step 12 - Configuration Complete** screen appears.

The Request Manager database is configured and the vCloud Director, Request Manager Admin Portal, and Active Directory settings are applied.

What to do next

Click Admin URL to access the Request Manager Admin Portal to make configuration changes and assign roles to users. Click Portal URL to access the Request Manager User Portal to view cloud and application inventory data.

Accessing Request Manager 4

You can access the Request Manager User Portal or the Request Manager Admin Portal, depending on your role and the tasks you need to perform.

The **Request Manager Admin Portal** is used by vCloud Administrators, Blueprint Administrators, and Asset Managers to perform management tasks. VMware vCloud Request Manager uses technology from VMware Service Manager. When you log into the vCloud Request Manager Admin Portal, it is labeled VMware Service Manager.

Asset Managers can use the Request Manager Admin Portal to perform tasks such as displaying software license inventory, adding software license inventory, and associating software licenses with vApp templates.

vCloud Administrators can use the Request Manager Admin Portal to perform post-installation configuration tasks, such as connecting to additional instances of VMware vCloud Director and changing security settings.

The **Request Manager User Portal** is used by engineers and cloud owners to request new cloud partitions and provision new virtual applications. See the *VMware vCloud Request Manager User's Guide*.

This chapter includes the following topics:

- "Access the Request Manager Admin Portal," on page 27
- "Access the Request Manager Admin Portal without Active Directory," on page 28
- "Access the Request Manager User Portal," on page 28

Access the Request Manager Admin Portal

Use a supported Web browser to launch the Request Manager Admin Portal.

Prerequisites

You have installed Request Manager.

Before you connect to the Request Manager Admin Portal, make sure that the service is running and you have a compatible Web browser. See "System Requirements," on page 15 for a list of supported Web browsers.

Procedure

1 Start your Web browser.

2 Enter the Request Manager Admin URL. `http://<hostname>/admin/`

3 In the Login window, enter your Request Manager user name and password and click **Login**.

The VMware Request Manager Admin Portal main window displays.

What to do next

See Chapter 5, "Administration Overview," on page 31 for administration tasks managed from the Admin portal.

Access the Request Manager Admin Portal without Active Directory

By default, administrators must access Request Manager Admin Portal using their Active Directory account credentials. If there are no administrator accounts in Active Directory, you can still log in to the Request Manager Admin Portal and assign users to an administrator role.

Request Manager provides a super-user account that can always access the Admin portal and promote new users to an administrator role vCloud Administrator, Blueprint Administrator, or Asset Manager).

The super-user account has fewer privileges than a regular administrator. This account should only be used to promote new administrators and allow further administration tasks to be performed by those users.

Procedure

1 Start your Web browser.

2 Enter the following URL:

```
http://<hostname>/admin/ServiceManager.aspx?NOAUTH=TRUE
```

Only the super-user account can log into this URL.

3 In the Login window, enter the super-user user name and password and click **Login**.

Option	Description
User name	Enter **ADMIN**.
Password	Enter the password specified when you configured the system identity in the configuration wizard. See "Configure Request Manager," on page 22.

What to do next

You can assign an administrator role to a user. See "Assign Roles to Users," on page 35.

Access the Request Manager User Portal

Use a supported Web browser to launch the Request Manager User Portal.

Prerequisites

You have installed Request Manager.

Before you connect to the Request Manager User Portal, make sure that the service is running and you have a compatible Web browser. See "System Requirements," on page 15 for a list of supported Web browsers.

Procedure

1 Start your Web browser.

2 Enter the Request Manager URL. `http://<hostname>/portal/`

3 In the Login window, enter your Request Manager user name and password and click **Login**.

Use your Active Directory credentials for your Request Manager user name and password.

The Request Manager application displays the contents of a single organization or cloud and lists the applications that are deployed in the current cloud.

What to do next

If you have access to multiple clouds (For example, if you are a member of multiple development teams or projects), you can switch between clouds using the cloud drop-down menu. You can switch between different filtered views of these applications using the filtering options on the toolbar. See the *VMware vCloud Request Manager User's Guide*.

Administration Overview 5

Use the Request Manager Admin Portal for system administration tasks.

This chapter describes how to use the Request Manager Admin Portal to configure Request Manager system settings for Active Directory, manage roles, connect to vCloud Director, change workflow and email notification settings, customize blueprints, and define providers.

This chapter includes the following topics:

- "Active Directory," on page 31
- "Request Manager Roles," on page 35
- "Connecting to Multiple Instances of VMware vCloud Director," on page 37
- "Incoming Email Server," on page 44
- "Workflow Management," on page 47
- "Cloud Blueprints," on page 57
- "Defining Providers," on page 59
- "Polling Service," on page 60

Active Directory

Request Manager populates user data by accessing the same Microsoft Active Directory domain used by vCloud Director.

In a default install, Request Manager's Active Directory server should be located within the same domain as vCloud Director's. Active Directory integration requires there is an existing single group or organization unit within the directory to which every user belongs. For example, Domain Users.

Active Directory users are imported as People in Request Manager. A person can be a Customer or an Officer - where an Officer has permissions to access the Request Manager Admin Portal for administration purposes.

Active Directory users are first imported into Request Manager during installation and configuration. Active Directory users that were selected as administrators during installation and configuration are Officers.

Configure Active Directory

During the installation of Request Manager, you created an Active Directory source. You can use the Request Manager Admin Portal to reconfigure your Active Directory settings.

Request Manager synchronizes users from the entire domain you specify in the LDAP server path. Synchronization with large domains can take a very long time. If only a subset of the users in a domain need to use Request Manger, VMware recommends that you configure the root naming context of the connection string to be specific to those users. For example, if all the required users reside in the Engineering organizational unit (OU) you could enter **`LDAP://.../OU=Engineering,dc=mydomain,dc=com`** for the connection string.

This will enable you to enforce security and restrict the users of Request Manager to its intended audience and also save you time synchronizing with Active Directory.

Prerequisites

- You have vCloud Administrator privileges.
- Request Manager has access to the Active Directory source.
- Request Manager is connected to a specific domain controller, not just a domain.

Procedure

1 Log in to the Request Manager Admin Portal.

2 Click **Integration.**

3 Click **Sources** on the **Main** tab in the left explorer panel.

4 Select Active Directory and click the **Select External Source** button.

5 Enter or modify the settings for the Active Directory source.

a Type a name to identify the Active Directory source.

b Select a status for the source.

Select **Active** to use the source throughout Request Manager. Select **Inactive** to disable the source throughout Request Manager.

c Type the full LDAP server path of the Active Directory server.

This must include the protocol, server, and root naming context and can optionally include a port number or a group of users. For example, `LDAP://myldapserver.mydomain.com:port/OU=mygroup/dc=mydomain,dc=com` or `LDAP://dc=mydomain,dc=com`.

You must use capital letters for the `LDAP` prefix.

For LDAP over SSL, type `LDAP://` for the server path and choose SSL.

d Type the user DN/ID.

This is the Windows account used to connect to the Active Directory server. You can type the user principal name, for example `login@domain`, or the flat domain name, for example, `domain\user`.

If you do not provide a User DN/ID, the connector uses the credentials of the executing accounts, in this case the Web server and Integration service. Ensure that both these accounts have appropriate rights.

e Type the password used to authenticate the user.

f If the connection string provides a specific server, select **Server Bind** for optimal performance.

Do not select this option for serverless connection strings.

g If the connection to Active Directory uses SSL, select **SSL**.

To use SSL, the Active Directory security certificate must be installed in the **Trusted Root Certification Authorities > Local Computer** folder.

h Select **Kerberos/NTLM** to use Kerberos/NTLM to authenticate the connection.

i Type the NT Domain Name of the Active Directory Server.

j Select **Authenticate Imported People against Source** to authenticate users logging into the Request Manager User Portal with their Active Directory credentials.

This options uses AD credentials and not the credential defined within Request Manager.

6 Click the **Test** button.

7 Click the **Save** button.

What to do next

Configure the Active Directory synchronization schedule.

Create or Modify an Active Directory Synchronization Schedule

vCloud Request Manager scans it associated Active Directory source daily. You can create a new schedule or modify and existing one to specify how often Request Manager scans the source.

Prerequisites

- You have vCloud Administrator privileges.
- Request Manager has access to the Active Directory source.

Procedure

1 Log in to the Request Manager Admin Portal.

2 Click **Integration.**

3 Click **Scheduling** on the **Main** tab in the left explorer panel.

4 Create a new schedule or modify an existing one.

To:	Action
Create a new schedule	Click **Add New Schedule**.
Modify an existing schedule	Select **Active Directory Scan** and click the **Select Schedule** button.

5 Type or modify the schedule details.

   a Type a name for the schedule.

   b Select a frequency for the scan.

   c Select the date and time for the next scan.

   d Select **Update All Records** to update information for every record in Active Directory, even those that have not changed since the last scan.

6 Click the **Sources** tab.

7 Click **Add** to add a source.

   a Select the Active Directory source you want to scan using this schedule.

   b Click **OK**.

8 Click **Save**.

What to do next

View the synchronization results.

View Active Directory Synchronization Activity

When a scheduled Active Directory scan runs, Request Manager updates the Activity log. You can view the log for information about the number of items discovered and updated, as well as the details for any errors.

Prerequisites

You have vCloud Administrator privileges.

Procedure

1 Log in to the Request Manager Admin Portal.

2 Click **Integration.**

3 Click **Scheduling** on the **Main** tab in the left explorer panel.

4 Select an Active Directory schedule and click **Select Schedule**.

5 On the **Activity** tab, select a scan and click **Open**.

6 Click the **Statistics** tab.

   This tab shows the number of resources scanned, updated, deleted, and so on.

7 Click the **Synchronization Log** tab.

   This tab displays errors logged during the scan. Double-click an error message to view more details.

Request Manager Roles

Request Manager uses roles to allow Active Directory users and groups control over Request Manager tasks and operations.

You identify your vCloud Admin, Blueprint Admin, and Asset Manager roles during installation planning. During installation, you assign these roles when you run the Request Manager configuration wizard.

After you install the Request Manager software, you can perform configuration settings to administrators using the Request Manager Admin Portal. You do not have to run the configuration wizard to manage administrators. To manage roles, you must log in the Request Manager Admin Portal as Administrator.

Roles

Request Manager enables access to functionality within the Admin portal using roles. Request Manager supports the following roles.

- General Access
- Workflow Management
- Configuration Management

Each role applies to any user who logs on to the Request Manager Admin Portal.

Users

Request Manager supports the following types of users.

- **Blueprint Administrator**. The Blueprint Administrator manages cloud blueprints, including creating and editing cloud blueprints. The Blueprint Administrator also manages Provider CIs, including creating and editing Providers and specifying the vCloud Director source, provider network, and the vCloud Director for that Provider CI.
- **Asset Manager**. The Asset Manager manages software products and licenses within the Admin portal. The Asset Manager receives inventory of new software licenses, and links software products to virtual applications.
- **Blueprint Admin/Asset Manager**. The Cloud Blueprint Admin and Asset Manager Security Role is a combination of the Cloud Blueprint Admin and the Asset Manager.
- **vCloud Administrator**. The vCloud Admin is the administrator responsible for Request Manager configuration after installation. The administrator is responsible for configuring the following.
  - Assigning security roles to cloud blueprint administrators and asset manager users.
  - Troubleshooting workflow tasks that fail to complete because of system errors.
  - Creating or editing workflow tasks to accommodate company-specific approval processes.
  - Managing integrated sources.

Assign Roles to Users

Use the Request Manager Admin Portal to assign administration roles to users.

VMware recommends that you assign the following roles to each type of user.

Table 5-1. Roles and Users

User	General Access Role	Workflow Management Role	Configuration Management Role
Blueprint Administrator	None	None	Blueprint Admin
Asset Manager	None	Asset Manager	Asset Manager
Blueprint Administrator/Asset Manager	None	None	Blueprint Admin and Asset Manager
vCloud Administrator	vCD Admin	vCD Admin	All

Prerequisites

- You have vCloud Administrator privileges.
- The user must already be imported into Request Manager.

Procedure

1 Log in to the Request Manager Admin Portal.

2 Click **People**.

The Person Search screen appears.

3 Specify the Person Search criteria in the left panel.

You need to specify at least one criterion in order to perform a search. You can type the wildcard character **%** in any text field to return all results for that criterion.

4 Click **Search.**

5 From the search results table, select a person and click the **Action** button.

6 Click the **Edit** button in the toolbar.

NOTE The Person Details record for this user is updated by Active Directory. You should take care not to modify pre-populated fields such as User ID, Object GUID, Manager, and so on.

7 Select **Officer**.

8 Select **Concurrent**.

9 On the **Security Roles** tab, assign the relevant security roles to the user.

Select a General Access role, Workflow Management role, and Configuration Management role.

10 On the **Workflow Groups** tab, assign the relevant workflow groups to the user.

Click **Selected** for each workflow group to which you want to assign this user. Click **Default WM** to set the user's default workflow management group. You can only assign one default workflow management group.

11 Click OK.

The Request Manager Person record is updated with the relevant details. The user can now log on to the Request Manager Admin Portal.

Connecting to Multiple Instances of VMware vCloud Director

You can connect to one or more instances of vCloud Director to Request Manager.

VMware vCloud Request Manager scans each instance of VMware vCloud Director to validate the list of Clouds, vApp Templates, and deployed vApps.

After you add a new instance of vCloud Director, you must configure Request Manager to use the new instance.

Add a vCloud Director Instance

If you want to import and manage virtual applications from more than one vCloud Director instance, you can add an instance.

Prerequisites

- You have vCloud Administrator privileges.
- Request Manager can access the vCloud Director instance.

Procedure

1 Log in to the Request Manager Admin Portal.

2 Click **Integration.**

3 Click **Sources** on the **Main** tab in the left explorer panel.

4 Click **Add New Source**.

5 Select **vCloud Connector** and click **OK**.

6 Enter the settings for the vCloud Director source.

   a Type a name to identify the vCloud Director source.

   b Select a status for the source.

   Select **Active** to use the source in Request Manager. Select **Inactive** to disable the source in Request Manager.

   c Type the URL for vCloud Director.

   For example, **`https://vCloudsystem.domain.com`**.

   Make sure to include **`https://`** as part of the URL. Do not include any path information that would access the vCloud Director console. For example, do not include **`/vcloud`** or **`/vcloud/myorg`** in the URL.

   To use SSL, the vCloud Director security certificate must be installed in the **Trusted Root Certification Authorities > Local Computer** folder.

   d Select **Bypass Proxy Settings** if you do not want to use the proxy server computer.

   This is useful if you are connecting to a computer on the local network.

   Occasionally proxy settings may prevent a connection being successfully established. Sometimes performance can vary depending on whether proxy settings are used or not.

   e Type the User ID to access vCloud Director.

   For example, **`Administrator@system`**. The user account must have system administrator privileges to vCloud Director.

   f Type the password used to authenticate the user.

7 Specify the fault detection and tolerance settings.

8 Select Send Fault Notifications if you want to send notifications to users.

   a Select **Always** of **After**.

     If you select **After**, type a number for failed attempts.

   b Click **Add** to add a recipient.

   c Select **People** or **Group**.

   d Type the name of a person or group and click **Find**.

   e Select the users or groups to notify and click **Add**.

   f Click **OK**.

9 Click the **Test** button to test the connection to vCloud Director.

   Request Manager reports if the test succeeds or fails.

10 Click the **Save** button.

What to do next

Configure resource mappings for the new instance of vCloud Director.

Configure Resource Mappings

After you add an instance of vCloud Director to Request Manager, you can create the resource mappings to specify the vCloud Director resources you can import from that instance.

In order to import mappings from instances of vCloud Director, you must define how the fields of entities in vCloud Director (such as virtual data centers, virtual applications, and so on) will map into Request Manager.

The following vCloud Director resource types must be mapped for each instance of vCloud Director . The list also shows the existing mapping that it has.

Table 5-2. Resource Mappings

vCloud Director Resource Type	Existing vCloud Request Manager Mapping Name
Catalog	Catalog
Catalog Item	Catalog Item vApp Template
Network	Cloud Network
Organization	Cloud
Provider Network	External Network
Provider vDC	Provider vDC
User	Cloud Members
vDC	vDC
vDC Resource > vApp	vApp
vDC Resource > vApp Template	vApp Template

Prerequisites

- You have vCloud Administrator privileges.
- You successfully added the vCloud Director instance.

Procedure

1 Log in to the Request Manager Admin Portal.

2 Click **Integration.**

3 Click **Resources** on the **Main** tab in the left explorer panel.

4 Select the vCloud Director source from the **Filter By Source** drop-down menu.

The list of available resources you can import from vCloud Director into Request Manager appears on the screen. Any resources that are already mapped into Request Manager display within a blue circle.

5 Double-click the resource you want to import.

6 Specify how the information from vCloud Director will be mapped to Request Manager.

VMware recommends that you copy the existing mappings defined in Request Manager for the vCloud Director source created during installation.

a Click **Clone From**.

b From the table, select the mapping you want to copy for this resource.

c Click **OK**.

Request Manager copies the details of the selected mapping and inserts it in the Mappings table.

7 Click the **Save** button.

Request Manager saves the mapping details for the selected resource and you will return to the Integration Resources screen. A blue circle will now display for the selected resource to indicate it is now mapped to Request Manager.

What to do next

Create link mappings.

Configure Link Mappings

After you configure the resource mappings for vCloud Director resources you can configure the link mappings.

In order to import mappings from instances of vCloud Director, you must define how the relationship among entities in vCloud Director (such as virtual data centers, virtual applications, and so on) map into Request Manager.

The following vCloud Director resource links must be mapped for each instance of vCloud Director . The list also shows the existing mapping.

Table 5-3. Link Mappings

vCloud Director Link Type	Import as Link Type
App Networks	vApp Networks
Catalog Contents	Service to Service Action
Network Association	Network Association
Organization Catalogs	Cloud Catalogs
Organization Networks	Cloud Networks
Organization vDCs	Cloud vDCs
Provider vDC Networks	Provider vDC Networks
vDC Available Networks	Available Networks
vDC Resources	vDC Resources

By default, all link types apply to parent mappings and child mappings.

Prerequisites

- You have vCloud Administrator privileges.
- You successfully added the vCloud Director instance.

Procedure

1 Log in to the Request Manager Admin Portal.

2 Click **Integration.**

3 Click **Links** on the **Main** tab in the left explorer panel.

4 Select the vCloud Director source from the **Filter By Source** drop-down menu.

A table of available links you can import from vCloud Director into Request Manager appears on the screen. Any resources which are already mapped into Request Manager will display with a selected checkbox in the Mapped column.

5 Double-click the link you want to import.

6 Specify how the information from vCloud Director will be mapped to Request Manager.

VMware recommends that you copy the existing mappings defined in Request Manager for the vCloud Director source created during installation.

Request Manager copies the details of the selected mapping and inserts it in the Mappings table.

7 Click the **Save** button.

Request Manager saves the mapping details for the selected link and you will return to the Integration Links screen. A checkmark will now display for the selected link to indicate it is now mapped to Request Manager.

What to do next

Create a vCloud Director synchronization schedule.

Create or Modify a vCloud Director Synchronization Schedule

When you add an instance of vCloud Director, you should include this additional instance into the schedule Request Manager uses when running a synchronization scan. You can create a new schedule for the instance or simply add the new vCloud Director instance to the schedule created during installation.

Synchronization scans VMware vCloud Director to validate the list of clouds, vApp Templates, and deployed vApps.

Apart for vCloud Director users, all vCloud Director entities are imported as CMDB items in Request Manager. The type of the CMDB items indicates the type of the vCloud Director entity.

Table 5-4. vCloud Directory Entities and Request Manager CMDB Types

vCloud Director Entity	Request Manager CMDB Type
Catalog	Service > Catalog
Catalog Item	Service Action > Catalog Item > Catalog vApp Template **Note** vApp templates are the only catalog items imported into Request Manager.
Network	Configuration Item > Cloud Network
Organization	Configuration Item > Cloud
Provider Network	Configuration Item > External Network

Table 5-4. vCloud Directory Entities and Request Manager CMDB Types (Continued)

vCloud Director Entity	Request Manager CMDB Type
Provider vDC	Configuration Item > Provider vDC
VM	Not imported
vDC	Configuration Item > Cloud vDC
vDC Resource	vDC Resources are imported as their specific types, for example, vApp.
Media	Not imported
vApp	Configuration Item > vDC Resource > vApp
vApp Template	Configuration Item > vDC Resource > vApp Template
User	When Request Manager synchronizes with vCloud Director, a match between vCD users and previously imported Active Directory users is performed. vCloud Director users that are created locally in the vCloud Director database or those that are created through importing from a non-Active Directory LDAP server will not be imported into Request Manager.

Prerequisites

You have vCloud Administrator privileges.

Procedure

1 Log in to the Request Manager Admin Portal.

2 Click **Integration.**

3 Click **Scheduling** on the **Main** tab in the left explorer panel.

4 Create a new schedule or modify an existing one.

To:	Action
Create a new schedule	Click **Add New Schedule**.
Modify an existing schedule	Select **Cloud Director Scan** and click the **Select Schedule** button.

5 Type or modify the schedule details.

   a Type a name for the schedule.

   b Select a frequency for the scan.

   c Select the date and time for the next scan.

   d Select **Update All Records** to update information for every record in vCloud Director, even those that have not changed since the last scan.

6 Click the **Sources** tab.

7 Click **Add** to add a source.

   a Select the vCloud Director source you want to scan using this schedule.

   b Click **OK**.

8 Click **Save**.

What to do next

View the synchronization results and create event mappings.

View vCloud Director Synchronization Activity

When a scheduled vCloud Director scan runs, Request Manager updates the Activity log. You can view the log for information about the number of items discovered and updated, as well as the details for any errors.

Prerequisites

You have vCloud Administrator privileges.

Procedure

1 Log in to the Request Manager Admin Portal.

2 Click **Integration.**

3 Click **Scheduling** on the **Main** tab in the left explorer panel.

4 Select a vCloud Director schedule and click **Select Schedule**.

5 On the **Activity** tab, select a scan and click **Open**.

6 Click the **Statistics** tab.

This tab shows the number of resources scanned, updated, deleted, and so on.

7 Click the **Synchronization Log** tab.

This tab displays errors logged during the scan. Double-click an error message to view more details.

Configure Event Mappings

In order to detect and import events from any additional instances of vCloud Director, you must define under what criteria to log an event in Request Manager, and how the fields of this event in vCloud Director will map into Request Manager.

This section outlines how you can set up event mapping to handle the return of a software license in Request Manager when the virtual application using this license is deleted from vCloud Director.

Prerequisites

- You have vCloud Administrator privileges.
- You successfully added the vCloud Director instance.

Procedure

1 Log in to the Request Manager Admin Portal.

2 Click **Integration.**

3 Click **Events** on the **Main** tab in the left explorer panel.

4 Select the vCloud Director source from the **Filter By Source** drop-down menu.

The list of available vCloud Director event types recognized by Request Manager appears on the screen. Any events that have defined how vCloud Director information translates into Request Manager has **Mapped** selected.

5 Select the event type you want to map and click the **Select Resource Type** button.

6 Specify how the information from vCloud Director will be mapped to Request Manager for the selected resource when an event is logged.

a Click New.

b Specify a name to identify the event type mapping.

The name for the default vApp Deleted event in Request Manager upon install is **Release Software Licenses**.

c Select **Log Request** in the **When Received** field.

This means whenever Request Manager detects the deletion of a virtual application from vCloud Director, a request will be logged within Request Manager.

d Use the **Using template** drop-down menu to specify the workflow template used to log the request.

Type `Release Software Licenses` and click the magnifying glass icon (search mode). The icon should now change to a page icon (details mode).

e Use the **Logging Officer** drop-down menu to specify the user responsible for any requests logged due to this event.

This user must have Officer selected on their Person Record. See "Assign Roles to Users," on page 35 for more information.

Type the last name of the user and click the magnifying glass icon. If there is a single match, the icon changes to a page icon. If there are multiple matches, a dialog displays a list of results. Select the user to add them to the field. The icon changes to a page icon.

7 Click the **Criteria** tab and select **Default Mapping** to log a request for every discovered event.

NOTE The default vApp Deleted event in Request Manager upon install has Default Mapping selected.

8 Click the **Action** tab to specify synchronization between the vCloud Director events and Request Manager requests.

For this drop-down	Select this value
When Updated externally	Update
When Updated externally and Call or Request is closed	Add note
When Notified externally	Add note
When Notified externally and Call or Request is closed	Add note
When Resolved externally	Close
When Resolved externally and Call or Request is closed	Add note
When Deleted externally	Close
When Deleted externally and Call or Request is closed	Add note

9 Click the **Fields - Incoming** tab to specify how fields from a vCloud Director event will map into Request Manager.

   a Click **Add** to create a field mapping.

   b Select **vApp** and click **OK**.

   This inserts a row in the Fields - Incoming table.

   c For the inserted internal field, select **Event Field**.

   d Select the tiers icon on the right of this cell to display a list of values.

   e Double-click **Resolution Rule**.

   f Select the tiers icon for **Please select a resolution rule**.

   g Double-click **Resolve vApp by vCD URL** so that it inserts into the field.

   h Click **OK** to insert the resolution rule into the Event Field.

   i In the **Update** drop-down menu, select **Always**.

10 Click the **Save** button.

   Request Manager saves the mapping details for the event and you will return to the Integration Events screen. The Mapped field is now selected for the event type to indicate it is now mapped to Request Manager.

What to do next

Refresh new Outbound Action Mappings for the additional instance of vCloud Director.

Refresh Outbound Action Mappings

Request Manager needs to refresh new Outbound Action Mappings for any additional instances of vCloud Director you create.

Prerequisites

You have vCloud Administrator privileges.

Procedure

1 Log in to the Request Manager Admin Portal.

2 Click **Integration.**

3 Click **Outbound Actions** on the **Main** tab in the left explorer panel.

4 Select the vCloud Director source from the **Filter By Source** drop-down menu.

   The list of available vCloud Director outbound action types recognized by Request Manager appears on the screen.

What to do next

Create a Provider. Create a Cloud Blueprint.

Incoming Email Server

During the installation of Request Manager, you provided information about the email server for incoming email. You can use the Request Manager Admin Portal to add a new incoming email server or modify the existing settings.

Request Manager supports POP3 (Post Office Protocol 3) and IMAP (Internet Message Access Protocol) for incoming email. After you set up an incoming email server, you can test the settings.

Add an IMAP Incoming Email Server

You can add an incoming email server that communicates using IMAP.

Procedure

1 In the Request Manager Admin Portal, open **System Administration > System > Email Settings**.

2 Click the **Add** button below the Incoming Email Servers section.

3 Select **IMAP**.

4 Specify the email server options.

Option	Action
Server	Enter the address used to connect to the IMAP server.
Port Number	Enter 143.
User ID	Enter the user name to connect to the mail server. Make sure that the account is set up on the mail server. Otherwise, Request Manager will not receive any incoming email.
Password	Enter the password to connect to the mail server.
Active	Select the check box. If you do not select it, Request Manager will not poll the system for incoming email.
Use SSL	Select this check box to specify that communications with the mail server should be over SSL.
Automatically select Authentication Method	Select this check box.
Deleted Items Folder	Enter `Deleted Items`.
Ignore Mail Server Report Messages	Select this check box.
Ignore On Blank Return Path	Select this check box.
Call Template	Select **Default**.
Default Logging Officer	This text box should specify **System Admin**. If it does not, use the Person Search window to locate and enter **System Admin**.
Use Linked Officer	Select this check box.

Make sure no other check boxes are selected.

5 Click **Save**.

What to do next

Test email settings.

Add a POP3 Incoming Email Server

You can add an incoming email server that communicates using POP3

Procedure

1 In the Request Manager Admin Portal, open **System Administration > System > Email Settings**.

2 Click the **Add** button below the Incoming Email Servers section.

3 Select **POP3**.

4 Specify the email server options.

Option	Action
Server	Enter the address used to connect to the POP3 server.
Port Number	Enter 110.
User ID	Enter the user name to connect to the mail server. Make sure that the account is set up on the mail server. Otherwise, Request Manager will not receive any incoming email.
Password	Enter the password to connect to the mail server.
Active	Select the check box. If you do not select it, Request Manager will not poll the system for incoming email.
Use SSL	Select this check box to specify that communications with the mail server should be over SSL.
Max Message per Session	Enter 10.
Automatically select Authentication Method	Select this check box.
Ignore Mail Server Report Messages	Select this check box.
Ignore On Blank Return Path	Select this check box.
Call Template	Select **Default**.
Default Logging Officer	This text box should specify **System Admin**. If it does not, use the Person Search window to locate and enter **System Admin**.
Use Linked Officer	Select this check box.

Make sure no other check boxes are selected.

5 Click **Save**.

What to do next

Test email settings.

Test Incoming Email Settings

After you configure the settings for an incoming email server, you can test the settings to make sure the connection is working.

Prerequisites

You have set up an incoming email server.

Procedure

1 In the Request Manager Admin Portal, open **System Administration > System > Email Settings**.

2 Select the outgoing email server and click **Test**.

3 Enter the **User ID** of the incoming email server in **To Address**, enter a subject and message, and click **OK**.

Request Manager reports on the status of the test.

4 Select the incoming email server and click **Test**.

Request Manager reports on the status of the test.

Workflow Management

This chapter provides an introduction to the implementation of workflows using the Request Manager Admin Portal Workflow Management module.

Workflow Templates

A Request is created in Request Manager when a consumer submits a request for an application or a cloud. Each request follows a pre-defined structure that includes the necessary tasks. The tasks are defined in Workflow Templates.

Request Manager provides three pre-defined Workflow Templates for enhanced governance and control of vCloud Director-based private clouds. You can modify these templates, but you cannot create new ones.

Provision vApp defines the process followed by requests to provision application. When a consumer submits a request for a vApp on the Request Manager User Portal, a request based on this Workflow Template is created. The process is:

- Consumer submits a request specifying the vApp Template, the name and description of the new vApp, the required expiry date of the new vApp and the target vDC.
- Request Manager emails the consumer's line manager to request approval to provision the vApp. If the request is declined, a notification email is sent to the consumer.
- When approval is obtained, any applicable software licenses are allocated to the vApp. Should there be no available licenses, notification emails are sent to the consumer, Asset Managers, and vCloud Administrators.
- The vApp is created in vCloud Director. Should provisioning fail, notification emails are sent to the consumer and vCloud Administrators. Any allocated software licenses are rolled back.
- When the vApp is successfully provisioned, the consumer receives a notification email.

Provision Cloud defines the process followed by requests to provision clouds. The process is:

- Consumer submits a request specifying Location, Blueprint, and the name and description of the new Cloud. Location and Blueprint are Request Manager CMDB items that must first be created by administrators before cloud provisioning can be performed. Location is the Provider CMDB item in Request Manager and defines the vCD instance, as well as provider vDC and network that the Cloud should be using. Blueprint defines the attributes of the new Cloud. See “Cloud Blueprints,” on page 57 and “Defining Providers,” on page 59 for more information on managing Providers and Blueprints.
- Request Manager emails the consumer's line manager to request for approval to provision the Cloud. If the request is declined, a notification email is sent to the consumer.
- When approval is obtained, the Cloud is created in vCD. Should provisioning fail, notification emails is sent to the consumer and vCloud Administrators.
- When the Cloud is successfully provisioned, the consumer is notified via email.

Release Software Licenses defines the process of releasing software licenses when vApps are deleted in vCloud Director. When a vCloud Director event that indicates a vApp being deleted is fielded by Request Manager, a request is created to update any software licenses that were taken up by the vApp.

These workflows can be configured in the following ways:

- Adding approvals at the beginning of a workflow. For example, in addition to line manager approval, finance approval is required for the provisioning of a cloud.
- Notifying a change management system when a vApp or cloud provisioning workflow is kicked off, or when the vApp or cloud has been successfully implemented in vCloud Director. This is done by adding a Run External Procedure task into the Workflow Template.
- Adding approval routing logic depending on the attributes of the request. For example, approvers for a new vApp may differ based on the destination vDC of the vApp. This is achieved by adding a Conditional Branching Task into the Workflow Template.

Modify Workflow Approvers

Workflow processes often require approvals to be given before the workflow can progress. You can change the approvers for a workflow.

Approvals restrict approval permissions to certain individuals and record details of the approval or rejection. Once an approval task is completed, the workflow progresses down certain dependency paths, based on whether it has been approved or rejected.

Multiple approvers can be assigned to an approval task in the Workflow Template. Once the task is activated, each approver assigned in the task receives an email. This email provides information on what needs to be approved and include mail-to links to approve or decline via email.

If a task is assigned to multiple approvers, a separate Customer Approval Task is created for each approver at run time. Each duplicated task will specify the approver that has been assigned the task.

Approvers can be added by specifying particular people or data fields. When data fields are used, approvers are assigned based on the values specified in the selected data fields when the task activates.

Prerequisites

You have vCloud Administrator privileges.

Procedure

1 Click **Workflow Template** in the Request Manager Admin Portal.

The Workflow Template Administration window appears.

2 Select a Workflow Template and click **Open**.

The Workflow Template Details window appears.

3 Click the **Dependencies** button.

The Task Dependencies window appears, displaying the workflow logic of the Workflow Template.

4 Double-click on the **Manager Approval** task.

The Customer Approval Details window appears.

5 To add more approvers, expand the Recipients section, and click **Add** under the Select Customers table.

The Recipients window appears.

6 To add specific people as approvers:

a Select **People**.

b Type all or part of the person's name and click **Find**.

You can type the wildcard symbol **%** to search for all people.

c Select the people to add as approvers and click **Add**.

7 To add a data field:

   a Select **Other**.

   b Select the fields to add as approvers and click **Add**.

   The Results table shows all People fields that are linked to the request, up to three levels. For example, Request No/Requestor refers to the person who submitted the request. Request No/Requestor/Manager refers to the manager of the person who submitted the request. The manager of a person is defined in the Person record. This information is imported from Active Directory.

8 Click **OK**.

9 To remove an approver, select an approver in the Recipients section and click **Delete**.

   A task must have at least one approver.

10 Click **Save**.

Modify Approval Emails

When a Customer Approval task is activated, approvers defined in the task receive emails. These emails provide information on what needs to be approved and includes links to approve or decline the request via email.

Do not modify approve and decline links in the email. Request Manager requires specific mail-to links to process the response emails from the approver.

Prerequisites

You have vCloud Administrator privileges.

Procedure

1 Click **Designer** in the Request Manager Admin Portal.

   The Designer window appears.

2 Select **Task** on the left of the window.

   A list of screens and message template appears on the right of the window.

3 To change the approval email for the Provision vApp Workflow Template, select **Provision vApp Approval** in Screen Set and **Message Template** in Screen Design.

4 Double-click **Provision vApp - Manager Approval** to open the message template.

5 To add a data field to the message template, select the field in the **Add a Field** tab on the left panel and drag-and-drop it onto the template.

   The **Data fields for** drop-down list shows the entities that the data fields are linked to. The list contains these values:

   - The entity associated with the currently opened message template. In this case the Customer Approval Task entity, Provision vApp Approval. Examples of Customer Approval Task data fields are Task Title, Task Description.
   - The Request entity that the Customer Approval Task is linked to, Provision vApp Approval's Request. Examples of Request data fields are vApp Name, vApp Description.
   - Sender and Recipient, which enables addition of fields relating to a person data, for example, First Name, Surname, Email ID and so on.

6 To remove a data field from the message template, select the field on the template, right click and select **Delete**.

7 To change the approval email for the Provision Cloud Workflow Template, select **Provision Cloud Approval** in Screen Set and **Message Template** in Screen Design.

8 Double-click **Provision Cloud - Manager Approval** to open the message template and modify the message template as described above.

Add an Approval Task to a Workflow Template

You can add a new approval task to the beginning or the end of the Provision vApp and Provision Cloud Workflow Templates. Multiple approvals can be arranged in a sequential or parallel manner in the workflow.

Prerequisites

You have vCloud Administrator privileges.

Procedure

1 Click **Workflow Template** in the Request Manager Admin Portal.

The Workflow Template Administration window appears.

2 Select a Workflow Template and click **Open**.

The Workflow Template Details window appears.

3 Click the **Dependencies** button.

The Task Dependencies window appears, displaying the workflow logic of the Workflow Template.

4 In the Task Dependencies window, select the Customer Approval Task from a palette of tasks and drag and drop it into the dependency diagram.

5 Link the task into the existing workflow.

a Hover over the task that precedes the new Customer Approval Task.

For example, Start Task.

b Click the link icon, drag the pointer to the Customer Approval Task, and release.

A grey arrow links the Start Task to the Customer Approval Task.

c Hover over the Customer Approval Task.

d Click the link icon and drag the pointer to the task that follows the Customer Approval Task in the workflow.

For example, Create vApp. A green arrow links the Customer Approval Task to Create vApp. A green arrow represents an Approved flow; when the Customer Approval Task results in an Approved state, the workflow will progress to Create vApp.

e To define a rejected flow, hover of the Customer Approval Task, click the link icon, and drag the pointer to another task.

For example, Notify Failed. A red arrow links the Customer Approval Task to Notify Failed. A red arrow represents a Rejected flow; when the Customer Approval Task results in a Rejected state, the workflow will progress to Notify Failed.

f You can change the state of a Customer Approval Task outgoing arrow by right-clicking on the arrow and selecting a different state.

In addition to Approved state and Rejected state, an arrow can have a Regardless state. In this case, the workflow will progress to the following task, regardless of the resulting state of the Customer Approval Task.

6 Double-click the Customer Approval Task to open it and enter the task details.

7 Specify the approval email that will be sent to the specified approver.

a Select **Screen Set** on the left of the Details window.

b Deselect **Use the default Screen Set** for Request and select a Screen Set from the list.

Request Manager provides two approval email templates out of the box. You can also define new email templates.

- Provision vApp Approval. If this Screen Set is selected, the approval email that is used by Manager Approval task in the Provision vApp Workflow Template will be used when the new Customer Approval Task is activated in a workflow.
- Provision Cloud Approval. If this Screen Set is selected, the approval email that is used by "Manager Approval" task in the Provision Cloud Workflow Template will be used when the new Customer Approval Task is activated in a workflow.

c Click **OK**.

d Click **Save**.

What to do next

If a new approval email for the task is required, save and exit the task, add a new message template and then link it to the task.

Add a New Approval Email Template

You can add a new approval email template to a Workflow Template.

Prerequisites

You have vCloud Administrator privileges.

Procedure

1 Open System Administration.

2 Select **Workflow Management** and then **Customer Approval Task Screen Set**.

3 Click **Add New Customer Approval Task Screen Set**.

The Task Screen Set Details window appears. Enter the screen set details. For example, select Provision vApp for the Request Screen Set if the new Customer Approval Task is for the Provision vApp Workflow Template.

4 Click **Save**.

5 Open Designer.

6 Select **Task** on the left of the window and click **Create**.

The Screen Details window appears.

7 Enter the screen details.

Option	Description
Create	Select Message Template.
Name	Enter a name for the new email template.

Option	Description
Screen Set	Select the Customer Approval Task Screen Set that you've created.
Copy From	Select the email template that you will use as the initial version of this new email template. For example, if the new email template is going to be similar to the existing vApp provisioning manager approval email, select Provision vApp Approval Provision vApp - Manager Approval.

8 Click **OK**.

The email template is created and is highlighted in the table of screens in the main window.

9 Double-click the new email template.

10 Assign the email template to the Customer Approval Task.

11 Open **System Administration**, select **System**, and click **Message Types**.

12 Search for Message Type 130 Task - Customer Approval.

13 Double-click the Message Type to open it.

The Message Type Map window appears.

14 Select the new email template and click **Add**.

15 Click in the Subject column and select the appropriate subject.

Workflow	Subject
Provision vApp	Provision vApp - Approval Request
Provision Cloud	Provision Cloud - Approval Request

16 Click **Save** in the toolbar.

What to do next

You can add a new approval task and link the email template to it. You can also link the email template to an existing approval task.

Assign Email Notification to Recipients

Notification emails are sent to various parties throughout the workflow. These emails inform the recipients of the status of a request. The recipients of these emails can be altered.

The steps below describe how to change the recipients of the Notify Declined email notification. You can follow similar steps to change the recipients for other email notifications.

Prerequisites

You have vCloud Administrator privileges and you have added new recipients as described in "Modify Workflow Approvers," on page 48.

Procedure

1 Double-click the task, Notify Declined.

The Messaging Task Details window appears

2 Click on the message template for the new recipient and select an existing message template from the drop-down list.

For example, select **Provision vApp - Notify Declined**.

3 Click **Save** on the Task Details window to save the changes you made to the task.

Change Email Notification Content

Notification emails are sent to various parties throughout the workflow. These emails inform the recipients of the status of a request. The content of these emails can be altered.

The steps below describe how to change the content of the Notify Declined email notification. You can follow similar steps to change the content for other email notifications.

Prerequisites

You have vCloud Administrator privileges.

Procedure

1 Click on **Designer** in the Request Manager Admin Portal.

The Designer window appears.

2 Select **Task** on the left of the window.

A list of screens and message templates appears on the right of the window.

3 Select **Base Task** in Screen Set and **Message Template** in Screen Design.

4 Double-click **Provision vApp - Notify Declined** to open it.

The message template appears.

5 To add or remove data fields to a message template see "Modify Approval Emails," on page 49.

The names of the message templates indicate which Workflow Template and tasks they are used in.

Templates with names starting with Provision vApp are used in the Provision vApp Workflow Template. It follows on for those with names starting with Provision Cloud and Release Software Licenses.

The second part of the name refers to the task for which the template is used. For examples, Provision vApp - Notify Declined is used in the vApp provisioning workflow task, Notify Declined; Provision vApp - Notify Success is used in the vApp provisioning workflow task, Notify Success.

Integrating External Tasks into a Workflow

The Run External Procedure Task allows you to automatically run an executable when the task is activated. It provides a level of integration through script files, web services, visual basic scripts and other executable files that would otherwise require customization within VMware Service Manager.

Invoking an executable within a workflow process provides the flexibility to make changes not only to other applications but also to networks, computers and hardware in the network, websites, configuration information, system setups and more.

Scripts are first added through the VMware Service Manager Server Console. Users can then specify any of these scripts to be run when a Run External Procedure Task becomes active in a workflow. Additional parameters can be passed from the Task or Request to the external task in order to fine tune the script. These parameters must be compatible with the selected script. Once the task is activated, the parameters will be appended to the script, the script will be run, the task will complete, and the workflow will progress.

Add an External Command to Service Manager

Before you can invoke an external command from within a workflow, you must add the external command to Service Manager.

Use the Service Manager Server Console to define the external commands that the Run External Procedure Task will reference. The Service Manager Server Console is installed on the Request Manager host machine when Request Manager is installed.

Prerequisites

You have vCloud Administrator privileges.

Procedure

1 Open the Service Manager Server Console.

2 Expand **System** and then click on **External Commands**.

3 Click **New External Command**, enter the details of the external command, and click **OK**.

Click the browse button to select an executable. The executable must be able to be run from the Request Manager host machine.

What to do next

Add a Run External Procedure Task to a workflow.

Add a Run External Procedure Task to a Workflow

You can add a Run External Procedure Task to a workflow to automatically run an executable when the task is activated.

Prerequisites

You have vCloud Administrator privileges and you have added an external command to the Service Manager Server Console.

Procedure

1 In the Task Dependencies window for a workflow, select the **Run External Procedure Task** from a palette of tasks and drag-and-drop it into the dependency diagram.

2 Link the task into the existing workflow, then double-click the task to open it.

3 Enter the task details.

In the **Command** field, select an executable that you defined in the Service Manager Server Console.

For more information about the **Parameters** field, see "Passing Field Values to a Run External Procedure Task," on page 54.

4 Click **Save**.

Passing Field Values to a Run External Procedure Task

You can pass field values to a Run External Procedure Task by using the Parameters field.

Field values from the request or task can be passed to the command by entering parameter names from the table into the Parameters field.

For example, to pass the constant, **vApp**, and the reference to a new vApp to a change management system, enter **[REQUEST:EXTFLDV_390022]**. The value of the vCloud Director Console URL for the vApp will replace **[REQUEST:EXTFLDV_390022]** in the command line of the external procedure task, for example `NotifyCM.exe vApp https://vcd1rhl5vcd.model.infra.com.au/api/v1.0/vApp/vapp-1386927350`.

Below is a list of data fields that can be passed as parameters to an external command. Square brackets **[** and **]** must be used in Parameters to indicate that the text refers to a data field.

Table 5-5. Common Request Data Fields

Reference	Field Description	Data Type
REQUEST:REQUEST_NO	Request No	Int
REQUEST:REQUEST_TITLE	Request Title	String

Table 5-5. Common Request Data Fields (Continued)

Reference	Field Description	Data Type
REQUEST:REQUEST_DESC	Request Description	Text
REQUEST:REQUESTOR_ REF $AR_PERSON.DISPLAY	Requestor	String
REQUEST:REQUESTOR_REF $AR_PERSON.EMAIL_ID	Requestor's Email Address	String
REQUEST:REQUESTOR_REF $AR_PERSON.USER_ID	Requestor User ID	String
REQUEST:EXTFLDV_390036$AR_PERSON.DISPLAY	Approver	String
REQUEST:EXTFLDV_390037	Approval Comments	Text

Table 5-6. Provision vApp Data Fields

Reference	Field Description	Data Type
REQUEST:EXTFLDV_390038$AR_PRIMARY_ASSET.DISPLAY	Target Cloud / Organization	String
REQUEST:SERVICE_REF $AR_PRIMARY_ASSET.DISPLAY	Catalog	String
REQUEST:SERVICE_ACTION_REF $AR_PRIMARY_ASSET.DISPLAY	Catalog Item	String
REQUEST:SERVICE_ACTION_REF $AR_PRIMARY_ASSET.EXTFLDV_390001$AR_PRIMARY_ASSET.DISPLAY	vApp Template	String
REQUEST:EXTFLDV_390024	vApp Title	String
REQUEST:EXTFLDV_390025	vApp Description	Text
REQUEST:EXTFLDV_390026	Required Until	Date/time
REQUEST:EXTFLDV_390027$AR_PRIMARY_ASSET.DISPLAY	Target vDC	String
REQUEST:EXTFLDV_390022	vApp URL in vCD Console. This will be populated only after the vApp has been successfully created in vCD.	String

Table 5-7. Provision Cloud Data Fields

Reference	Field Description	Data Type
REQUEST:EXTFLDV_3900028$AR_PRIMARY_ASSET.DISPLAY	Provider/Location	String
REQUEST:EXTFLDV_3900028$AR_PRIMARY_ASSET.EXTFLDV_390008$AR_PRIMARY_ASSET.DISPLAY	Provider vDC	String
REQUEST:SERVICE_ACTION_REF $AR_PRIMARY_ASSET.DISPLAY	Cloud Blueprint	String
REQUEST:EXTFLDV_3900030	Cloud Title (User-friendly)	String
REQUEST:EXTFLDV_3900031	Cloud Description	Text

Table 5-7. Provision Cloud Data Fields (Continued)

Reference	Field Description	Data Type
REQUEST:EXTFLDV_3900039	Cloud Name (Unique)	String
REQUEST:EXTFLDV_390022	Cloud/Organization URL in vCD Console. This will be populated only after the Cloud has been successfully created in vCD.	String

Add a Conditional Branching Task to a Workflow

Conditional Branching allows the configuration of a set of rules that control the progress of a workflow. For example, you could use conditional branching to route approvals depending on the target vDC of a new vApp.

Prerequisites

You have vCloud Administrator privileges.

Procedure

1 In the Task Dependencies window for a workflow, select the **Conditional Branching Task**from a palette of tasks and drag-and-drop it into the dependency diagram.

2 Link the task into the existing workflow, then double-click the task to open it.

3 Enter the task details.

4 To create a rule, click **New Rule**.

The Rule Setup section appears in the window.

5 To create a new Condition, click **Create Condition** in the If Available Conditions panel. The Available Conditions box appears. Enter the details of the condition, click **Add to List** and then **Save**.

The Select an Item drop-down contains the fields that are used as criteria for a condition. For example, Target vDC.

6 To create a new action, click **Create Action**. The Task/Approval Available Actions window appears. Enter the details of the action. Click **Add to List** and **Save**.

For example, select Customer Approval Forward to Customer in the Select an Item drop-down. This forwards the following Customer Approval Task to the person specified in **Customer**.

7 Select all the criteria for Rule Setup and then click **Add Rule**.

The Rule Setup window closes and the rule is added to the Rules list.

8 In the Task Details window, click **Save**.

Configure Request Completion Statuses

You can add, delete, and change the order of request completion statuses.

You cannot delete the **Unspecified** request completion status and VMware recommends that you do not rename it.

Prerequisites

You have vCloud Administrator privileges.

Procedure

1 Open System Administration, select **Workflow Management**, and click **Request Completion Statuses**.

The Request Completion Statuses window appears.

2 To create a new request completion status:

a Click **Add**.

b Type in the name of the new status in the **Name** column.

c If you want to the status to be available in the Closure Task, select the **Closure** checkbox.

d Click **Save**.

3 To delete a request completion status:

a Click **Delete**.

b Click **Save**.

4 To change the display order of the statuses:

a Select an entry and use the **Move Up** and **Move Down** buttons.

b Click **Save**.

What to do next

Configure Workflow Templates.

Cloud Blueprints

Cloud Blueprints define the characteristics of a cloud to ensure certain settings are enforced when the cloud is created. Examples of these settings are: the number of virtual machines allowed, the allocation model used, and quotas and limits for the Storage, CPU, Memory, Network, and so on. A Cloud Blueprint must be specified by the consumer when requesting a new cloud in the Request Manager User Portal.

The benefits of Cloud Blueprints include:

- Requests for cloud provisioning are vastly simplified as the consumer does not need to understand the details of cloud settings.
- Administration of these clouds is vastly simplified as the number of variations in the environment is greatly reduced.

Create a Cloud Blueprint

Use Request Manager to create a Cloud Blueprint.

Prerequisites

You must be have Blueprint Administrator or vCloud Administrator privileges.

Procedure

1 Click **CMDB Items** in the Request Manager Admin Portal.

The New CMDB Item window appears.

2 Select **Cloud Blueprint TEMPLATE** and click **Create from Template**.

The Cloud Blueprint Details window appears.

3 Enter details of the Cloud Blueprint.

Depending on the allocation model selected, the percentage of resources guaranteed need to meet certain conditions for the request to provision the cloud to complete successfully.

Allocation Model	Conditions
Pay-As-You-Go	Values for % Resources Guaranteed for CPU and memory must be > 0.
Allocation Pool	Values for % Resources Guaranteed for CPU and memory, CPU (GHz), and Memory (GB) must be > 0.
Reservation Pool	Values for % Resources Guaranteed for CPU and memory, CPU (GHz), and Memory (GB) must be > 0.

4 Click **OK** to save your changes and close the window.

The Cloud Blueprint is now available to consumers when requesting a cloud in the Request Manager User Portal.

Edit a Cloud Blueprint

Use Request Manager to edit a Cloud Blueprint.

Prerequisites

You must be have Blueprint Administrator or vCloud Administrator privileges.

Procedure

1 Click **CMDB Items Search** in the Request Manager Admin Portal.

2 Click the List icon on the right of the search criterion, **CMDB Item Type**.

3 Select **Service Action** and double-click on **Cloud Blueprint** on the second panel.

Cloud Blueprint is entered in CMDB Item Type and the search criterion is selected.

4 Click **Search** at the bottom of the search criteria panel.

The search results are shown on the right of the window.

5 Double-click the Cloud Blueprint you wish to edit.

The Cloud Blueprint Details window appears.

6 Modify the details of the Cloud Blueprint and click **OK** to save the changes and close the window.

You may have to click **Edit** on the toolbar.

Delete a Cloud Blueprint

Use Request Manager to delete a cloud blueprint.

Prerequisites

You must be have Blueprint Administrator or vCloud Administrator privileges.

Procedure

1 Search for the Cloud Blueprint using CMDB Item Search.

2 Select the Cloud Blueprint to delete and click **Delete** on the search toolbar.

The Cloud Blueprint is deleted and no longer available to consumers when requesting a cloud in the Request Manager User Portal.

Defining Providers

To provision a new cloud, a provider vDC and provider network must be specified. These are specific to a single vDC instance. A Provider in Request Manager points to a specific vDC instance, provider vDC and provider network, thus simplifying the process of cloud provisioning for the consumer by masking the details of the location of the cloud.

Create a Provider

Create a Provider to simplify the process of cloud provisioning.

Prerequisites

You must be have Blueprint Administrator or vCloud Administrator privileges.

Procedure

1 Click **CMDB Items** in the Request Manager Admin Portal.

The New CMDB Item window appears.

2 Select **Provider TEMPLATE** and click **Create from Template**.

The Provider Details window appears.

3 Enter details of the Provider.

Option	Description
vCD Source	Shows all vCloud Director sources that Request Manager is connected to.
Provider vDC	Shows the provider vDCs of the selected vCD Source.
Provider Network	Shows the provider networks of the selected vCD Source.

4 Click **OK** to save changes and close the window.

The Provider is now available to consumers when requesting for a cloud in the Request Manager User Portal.

Edit a Provider

Edit a Provider to change its settings.

Prerequisites

You must be have Blueprint Administrator or vCloud Administrator privileges.

Procedure

1 Click **CMDB Items Search** in the Request Manager Admin Portal.

2 Click the list icon on the right of the search criterion, **CMDB Item Type**.

3 Select **Configuration Item** and double-click on **Provider** on the second panel.

Provider is entered in CMDB Item Type and the search criterion is selected.

4 Click **Search** at the bottom of the search criteria panel.

The search results are shown on the right of the window.

5 Double-click the Provider you wish to edit.

The Provider Details window appears.

6 Modify the details of the Provider and click **OK** to save the changes and close the window.

You may have to click **Edit** on the toolbar.

Delete a Provider

Delete a Provider to make it unavailable for cloud provisioning.

Prerequisites

You must be have Blueprint Administrator or vCloud Administrator privileges.

Procedure

1 Search for the Provider using CMDB Item Search.

2 Select the Provider to delete and click **Delete** on the search toolbar.

The Provider is deleted and no longer available to consumers when requesting for a cloud in the Request Manager User Portal.

Polling Service

Request Manager installs the polling service automatically. You can see this running from the web server under the Services Console.

The following table lists relevant services and provides a brief description of the tasks each service performs. Services run every 60 seconds, except the Workflow service which runs every 3 seconds.

Table 5-8. Polling Service

Service	Description	Default Timeout
Administrative	Parent service for all Request Manager services.	0
Connector	Service for connectors.	0
Messaging	Service for sending emails.	15
Workflow	Service for activating tasks in the Workflow.	20

Stop a Polling Service

You can manually stop a polling service.

Procedure

1 Select the **Control Panel** option from the Windows Start menu.

The Windows Control Panel appears.

2 Select **Administrative Tools > Services**.

3 Right-click the service you want to stop and select **Stop** from the menu.

About Software License Management 6

This chapter describes how to use the Request Manager Admin Portal to configure Request Manager system settings for linking software licenses to vApp templates and adding license information to a software product.

This chapter includes the following topics:

- "Understanding Licenses," on page 61
- "Create a Software Product," on page 61
- "Edit a Software Product," on page 62
- "Delete a Software Product," on page 62
- "Add License Information to a Software Product," on page 63
- "Defining Software Products Options," on page 63
- "Viewing Software License Allocation," on page 65
- "Associating Software Products with vApp Templates," on page 66

Understanding Licenses

Software license management guarantees license compliance and optimizes license utilization. Software Product records help you manage your licenses for that particular software. For example, you can have a Software Product record for Microsoft Windows 7 and manage all the licenses you own for this product from the single record.

Request Manager provides nine Software Product records out of the box. You can edit these records, as well as add new Software Products.

Create a Software Product

You can create a Software Product to help manage licenses for a particular product.

Prerequisites

You have Asset Manager privileges.

Procedure

1 Click **CMDB Items** in the Request Manager Admin Portal.

The New CMDB Item window appears.

2 Click the list icon on the right of **CMDB Item Type**.

3 Select **Configuration Item** and double-click **Software Product** on the second panel.

Software Product is entered in CMDB Item Type.

4 Click **Create**.

The Software Product Details window appears.

5 Enter details of the Software Product.

See "Defining Software Products Options," on page 63 for more information about configuring values for **Manufacturer** and **Asset Lifecycle Status**.

6 Click **OK** to save the changes and close the window.

What to do next

Add license information to the Software Product.

Edit a Software Product

Use Request Manager to edit a Software Product.

Prerequisites

You have Asset Manager privileges.

Procedure

1 Click **CMDB Items Search** in the Request Manager Admin Portal.

2 Click the List icon on the right of the search criterion, **CMDB Item Type**.

3 Select **Configuration Item** and double-click on **Software Product** on the second panel.

Software Product is entered in CMDB Item Type and the search criterion is selected.

4 Click **Search** at the bottom of the search criteria panel.

The search results are shown on the right of the window.

5 Double-click the Software Product you wish to edit.

The Software Product Details window appears.

6 Modify the details of the Software Product and click **OK** to save the changes and close the window.

You may have to click **Edit** on the toolbar.

Delete a Software Product

Use Request Manager to delete a Software Product.

Prerequisites

You have Asset Manager privileges.

Procedure

1 Search for the Software Product using CMDB Item Search.

2 Select the Software Product to delete and click **Delete** on the search toolbar.

Add License Information to a Software Product

You can add, update, or delete the license information associated with a Software Product.

Prerequisites

You have Asset Manager privileges.

Procedure

1 Open a Software Product Details window.

2 Click **Licenses** on the left of the window, expanding it if required, and then click **Transactions**.

The Transactions window appears.

3 To enter new licenses for the software, click **New** on the Purchases tab.

The New Purchase window appears.

4 Enter the number of new licenses in **Quantity**.

5 Click **OK** to save the changes and close the window.

The purchase displays in the Purchases List and the On Hand list. On Hand licenses are available to be allocated to a vApp template.

6 To update a Purchase, click **Update** at the bottom of the Purchases list.

The Update Purchase window appears.

7 Change the quantity and then click **OK** to save the changes and close the window.

A Purchase cannot be updated if some of the licenses in that Purchase record are in use.

8 To delete a Purchase, click **Delete** at the bottom of the Purchases list.

A Purchase cannot be deleted if some of the licenses in that Purchase record are in use.

What to do next

Associate software products to vApp Templates.

Defining Software Products Options

You can define the manufacturers and asset lifecycle status for Software Products.

Define Manufacturers

You can create, edit, or delete a Manufacturer.

Prerequisites

You have Asset Manager privileges.

Procedure

1 In the System Administration window, under the CMDB section, click **Manufacturers**.

The Manufacturers window appears.

2 To create a manufacturer:

a Click **Add New** on the toolbar.

A new row is added to the table.

b Type the name of the manufacturer.

3 To edit a manufacturer:

a Select the manufacturer you want to edit.

b Click within the entry such that the row is editable.

c Change the name of the manufacturer.

4 To delete a manufacturer:

a Select the manufacturer you want to delete.

b Click **Delete** on the toolbar.

5 Click **Save**.

Define Asset Lifecycle Status

You can create, edit, or delete an Asset Lifecycle Status

Prerequisites

You have Asset Manager privileges.

Procedure

1 In the System Administration window, under the CMDB section, click **Asset Management - Asset Lifecycle Status**.

The Asset Lifecycle Status window appears.

2 To create an asset lifecycle status:

a Click **Add New** on the toolbar.

A new row is added to the table.

b Type the name of the status

c To specify the status as the one that is first displayed for new Software Products, select the checkbox in the Default column.

3 To edit a status:

a Select the status you want to edit.

b Click within the entry such that the row is editable.

c Change the name of the status.

4 To delete a status:

a Select the status you want to delete.

b Click **Delete** on the toolbar.

5 Click **Save**.

What to do next

Create new Software Products.

Viewing Software License Allocation

When a vApp is created in vCloud Director via Request Manager, software licenses that are associated to the vApp Template used to create the vApp are allocated to the new vApp.

When a vApp is deleted in vCloud Director, Request Manager releases all software licenses allocated to the vApp. The allocation record is removed and the available license count for that software is increased.

View Summary of Allocations

You can view a snapshot of the number of licenses that remain available/on hand and the number already allocated.

Prerequisites

You have Asset Manager privileges.

Procedure

1 Open a Software Product and browse to the **Item Summary** section.

2 View the number of items under the corresponding allocation pools.

View Available Software Licenses

You can view the licenses available to a Software Product.

Prerequisites

You have Asset Manager privileges.

Procedure

1 Open a Software Product and navigate to the licensing section.

2 Click the **On Hand** tab.

The On Hand List displays all available licenses for the software product.

View In Use Software Licenses

You can view the vApps that are consuming the software licenses for a Software Product.

Prerequisites

You have Asset Manager privileges.

Procedure

1 Open a Software Product and navigate to the licensing section.

2 Click the **In Use** tab.

The In Use List displays all vApps that are consuming licenses of the software product.

3 Click **Filter Columns**.

The Column Configs window is displayed.

4 Select **CMDB Item** in the Visible Columns list and click the up arrow or down arrow to position the column so that it is visible in the In Use List.

5 Click **OK**.

The vApp to which the license is allocated is now visible in the In Use List.

View Transaction History

Each time a software license is allocated or released from a vApp, a record is added to the asset management transaction history. You can view this history.

For information about setting the number of transactions displayed, see "Set Browse Limits," on page 66.

Prerequisites

You have Asset Manager privileges.

Procedure

1 Click **Transaction History** on the left of the Software Product Details window.

The Transaction History window appears. The top of the window displays a series of filter criteria and the bottom is a table that displays asset management transactions that match the criteria above.

2 Click **Filter Columns** to change the visibility of the columns in the results table, as well as the order in which the columns appear.

3 Select and specify one or more criteria in the top section and click **Refresh** on the toolbar.

The transactions that match your criteria are displayed in the table below.

The number of records shown in the table is determined by a system administration setting. If the limit has been set to 1000, only 1000 rows are displayed in the results table.

4 To filter the results by a value in the column, click on the down arrow on the column heading.

Set Browse Limits

You can set the maximum number of records to display in a Transaction History results table.

Procedure

1 Click System Administration in the Request Manager Admin Portal.

2 Click **System > Browse Limits**.

3 Enter the number of records you would like the Transaction History results table to show in **CMDB Search**.

This setting also determines the number of records shown when searching for CMDB Items.

Associating Software Products with vApp Templates

You can use Request Manager to search for all vApp templates, search for vApp templates that do not currently have any software products associated with them, and to update the software products associated with a vApp template.

Search for all vApp Templates

You can search for all vApp templates and then update the Software Products associated with a vApp template.

See "Update the Software Products Associated with a vApp Template," on page 68 for information about associating Software Products to a vApp template.

Prerequisites

You have Asset Manager privileges.

Procedure

1 Click **CMDB Items Search** in the Request Manager Admin Portal.

The CMDB Item Search window appears.

2 In CMDB Search Criteria, click the list icon next to **CMDB Item Type** and select **Configuration Item > vDC Resource > vApp Template**.

vApp Template is inserted into CMDB Item Type and CMDB Item Type is selected.

3 Select **Equal + Below**.

4 Click **Search**.

The search results appear on the right hand side.

5 Double-click on any of the search result to view the details of the vApp Template.

You can also select **Action** on the search result toolbar after selecting a vApp Template in the results table.

The vApp Template Details window appears.

What to do next

Update the software products that are associated to a vApp Template.

Search for vApp Templates With Software Product Association

You can search for all vApp templates with a Software Products association and then update the Software Products associated with the vApp template.

See "Update the Software Products Associated with a vApp Template," on page 68 for information about associating Software Products to a vApp template.

Prerequisites

You have Asset Manager privileges.

Procedure

1 Click **CMDB Items Search** in the Request Manager Admin Portal.

The CMDB Item Search window appears.

2 Click **Configure Search Criteria** on the CMDB Search Criteria toolbar.

The Search Criteria Configuration window appears.

3 Type **`VM Software Licenses`** in Section Name and click **Create Section**.

VM Software Licenses appears on the right-side.

4 In the list of criteria on the left-side to locate the fields titled, VM Software Licenses, select them all, and click **Add to Section**.

The fields are added to the right Visible Criteria column under VM Software Licenses.

5 Click **Move Up** or **Move Down** to position the section on the criteria panel.

6 Click **OK**.

The Search Criteria Configuration window is closed. The CMDB Search Criteria is updated.

7 Enter all or part of the title of the Software Product that is associated to the vApp Template in one of the VM Software Licenses criteria and press **Enter**.

The CMDB Item Quick Search window appears with a list of CMDB Items with the title you entered.

8 Double-click the software product that is associated with the vApp Template.

The Software Product is entered into the search field.

9 There may be other CMDB Items that match the search value but are not Software Products. To filter the results to Software Products, click the **Columns** icon on the Quick Search toolbar.

The Column Configs window appears.

10 Select **CMDB Item Type** from the Hidden Columns list and click the arrow key to move it to the Visible Columns list.

11 Click the up arrow or down arrow to position the field in the table.

12 Click **Apply** and then click **OK**.

The Column Configs window is closed and the Quick Search window is updated.

13 Click on the **CMDB Item Type** column header to expand it.

A list of available CMDB Item Type in the result list is shown.

14 Select **Software Product**.

The result table is updated to show only Software Products.

15 Enter `vApp Template` in **CMDB Item Type** and select **Equal + Below**.

16 Click **Search**.

The search results appear on the right side.

17 Double-click any of the search result to view the details of the vApp Template.

You can also select **Action** on the search result toolbar after selecting a vApp Template in the results table.

The vApp Template Details window appears.

What to do next

Update the software products that are associated to a vApp Template.

Update the Software Products Associated with a vApp Template

You can add and remove Software Products from a vApp template.

Prerequisites

You have Asset Manager privileges.

Procedure

1 On a vApp Template Details window, enter a Software Product in one of the multi-value QD fields titled, VM Software Licenses.

You can add multiple Software Products into each VM Software Licenses field.

2 To remove a Software Product, select the Software Product and click the remove icon.

The selected Software Product is removed from the VM x Software Licenses field.

3 Click **OK**.

What to do next

Index

A

accessing Request Manager **27, 28**
Active Directory
  configuring **32**
  overview **31**
  synchronization results **34**
  synchronization schedule **33**
approval email, adding **51**
approval task, adding **50**
approving workflows **48**
asset management, transaction history **66**

B

browse limits, setting **66**

C

cloud blueprints
  creating **57**
  deleting **58**
  editing **58**
  overview **57**
conditional branching **56**
cookies **20**

E

educational support **5**
email approvals for workflow **49**
email notification
  modifying message content **53**
  recipients **52**
email server
  adding IMAP **45**
  adding POP3 **45**
  test settings **46**
external commands, adding **53**
external tasks **53**

F

finding more information **13**

I

installation, planning worksheet **12**
installation overview **21**

L

licenses, about **61**

N

network ports **11**

O

Oracle Server, configuration **17**
outbound action mapping **44**

P

passing field values **54**
performance **18**
planning worksheet, installation **12**
polling service, stopping **60**
preparing to use **11**
providers
  creating **59**
  deleting **60**
  editing **59**
  overview **59**

R

request completion status **56**
Request Manager
  about **7**
  accessing **27**
  accessing Admin Portal **27**
  accessing User Portal **28**
  configuration wizard **22**
  installing **21**
Request Manager, accessing **28**
roles, assigning **35**
Run External Procedure tasks **54**

S

scalability, database **18**
scanning LDAP, performance **18**
scanning vCloud Director, performance **18**
security certificates
  Active Directory **19**
  installing **20**
  vCloud Director **19**
  warnings **20**
software licenses
  allocation **65**
  available **65**
  in use **65**

managing **61**
overview **65**
software products
adding license information **63**
asset lifecycle status **64**
associating vApp templates **66**
creating **61**
deleting **62**
editing **62**
manufacturers **63**
options **63**
System Administration, overview **31**
system components **7**
system requirements **15**

T

technical support **5**

V

vApp templates
associating Software Products **68**
search for all **66**
with Software Product associations **67**
vCloud Director
adding an instance **37**
configuring event mappings **42**
configuring link mappings **39**
configuring resource mappings **38**
multiple instances **37**
synchronization results **42**
synchronization schedule **40**

W

workflow approval email **49**
workflow approvers **48**
workflow management **47**